

10/756, 893

PAT-NO: JP02002259866A

DOCUMENT-IDENTIFIER: JP 2002259866 A

TITLE: CARD READER DEVICE OF TYPE CONNECTED TO
PORTABLE
SETTLEMENT
TERMINAL AND METHOD OF AUTHENTICATION AND
USING IT

PUBN-DATE: September 13, 2002

INVENTOR-INFORMATION:

NAME	COUNTRY
YOSHIDA, KIYOHICO	N/A

INT-CL (IPC): G06F017/60, G06K017/00 , G07F007/10 , G09C001/00 ,
H04L009/08

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a card reader device preventing bugging of card information as to credit cards or the like and ID numbers, and illegal copies and use, and a method of authentication and settlement using the device.

SOLUTION: A store notifies the host computer 3 of a bank or the like of the price of merchandise and the telephone number of the portable terminal 2 of a card user. The host computer 3 creates a public key and a secret key and calls up the portable terminal 2 of the card user to transmit the public key. The portable terminal 2 transmits the received public key to the card reader device 1 connected thereto. Using the public key received, the card reader device 1 encrypts the read card information and ID number for transmission to the portable terminal 2 connected thereto. The portable terminal 2 transmits to the host computer 3 the encrypted card information and ID number transmitted from the card reader device 1. The host computer 3 decrypts the

encrypted card
information and ID number with the secret key corresponding to the
public key
to carry out a settlement process.

COPYRIGHT: (C) 2002, JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-259866

(P2002-259866A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)	
G 0 6 F 17/60	4 1 4	G 0 6 F 17/60	4 1 4	3 E 0 4 4
	Z E C		Z E C	5 B 0 5 8
	2 2 4		2 2 4	5 J 1 0 4
	2 3 2		2 3 2	
	2 4 2		2 4 2	

審査請求 有 請求項の数 6 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願2001-52350 (P2001-52350)

(22) 出願日 平成13年2月27日 (2001.2.27)

(71) 出願人 000232254

日本電気通信システム株式会社

東京都港区三田1丁目4番28号

(72) 発明者 吉田 清彦

東京都港区三田1丁目4番28号 日本電気
通信システム株式会社内

(74) 代理人 100065385

弁理士 山下 稔平

Fターム (参考) 3E044 BA04 DA06

5B058 CA27 KA02 KA04 KA08 KA35
YA02

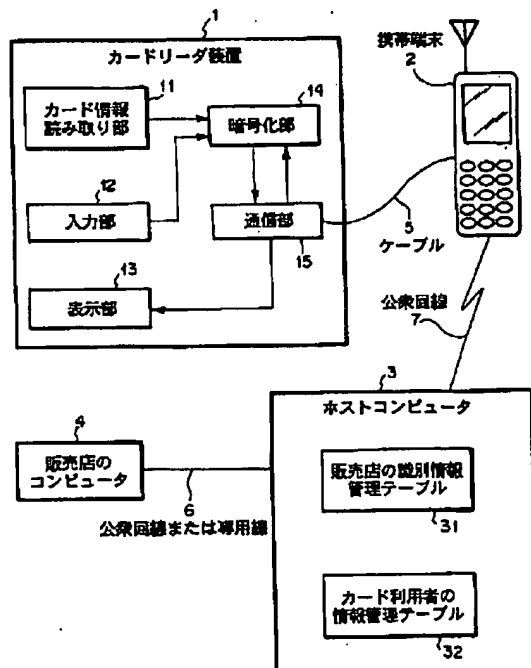
5J104 AA04 AA07 AA13 KA01 KA05
KA21 MA01 NA05 PA02 PA10

(54) 【発明の名称】 携帯端末接続型カードリーダ装置及びそれを用いた認証決済方法

(57) 【要約】

【課題】 クレジットカード等のカード情報や暗証番号の盗聴及び不正コピー、不正使用を防ぐカードリーダ装置及びそれを用いた認証決済方法を提供する。

【解決手段】 販売店は商品の代金とカード利用者の携帯端末2の電話番号を銀行等のホストコンピュータ3に通知する。ホストコンピュータ3で公開鍵と秘密鍵を生成して、カード利用者の携帯端末2に電話して公開鍵を送信する。携帯端末2は、接続されたカードリーダ装置1に受け取った公開鍵を送る。カードリーダ装置1は、読み込んだカード情報や暗証番号を、受け取った公開鍵を使って暗号化して、接続された携帯端末2に送る。携帯端末2は、カードリーダ装置1から送られた暗号化されたカード情報や暗証番号を、ホストコンピュータ3に送る。ホストコンピュータ3では、暗号化されたカード情報や暗証番号を公開鍵に対応する秘密鍵で復号化して決済処理を行う。



【特許請求の範囲】

【請求項1】 ケーブルにより携帯端末に接続されたカードリーダ装置であって、
カードの情報を読み取るカード情報読み取り部と、
暗証番号を入力するための入力部と、
前記カード情報読み取り部で読み取ったカード情報及び
前記入力部から入力された暗証番号を暗号化する暗号化
部と、
この暗号化部により暗号化されたカード情報及び暗証番
号をケーブル接続された前記携帯端末に送信する通信部
と、
操作を促すメッセージを表示する表示部と、を備えるこ
とを特徴とするカードリーダ装置。

【請求項2】 前記暗号化部において公開鍵暗号化方式
により暗号化を行うことを特徴とする請求項1記載のカ
ードリーダ装置。

【請求項3】 前記暗号化部で暗号化を行う際に使用す
る公開鍵を、前記通信部によりケーブル接続されている
前記携帯端末を介して外部から受け取ることを特徴とす
る請求項2記載のカードリーダ装置。

【請求項4】 請求項1に記載されたカードリーダ装置
を用いた認証決済方法であって、
販売店の端末からカード発行元のホストコンピュータ
に、カード利用者の携帯端末の電話番号、販売店の識別
情報、商品の金額情報を通知し、
前記ホストコンピュータは、前記携帯端末から電話回線
を介して前記カードリーダ装置で読み取ったカード情報
及び暗証番号を受信し、
受信したカード情報及び暗証番号を使って認証を行うこ
とを特徴とする認証決済方法。

【請求項5】 カード発行元のホストコンピュータか
ら、前記カードリーダ装置に接続された前記携帯端末を
介して、公開鍵暗号化方式による暗号化に用いる公開鍵
を配布し、
前記カードリーダ装置の暗号化部で、前記カード情報及
び暗証番号を前記配布された公開鍵を用いて暗号化する
ことを特徴する請求項4記載の認証決済方法。

【請求項6】 前記暗号化部で使用する公開鍵を、認証
決済処理の度に更新することを特徴する請求項5記載の
認証決済方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、携帯電話やPHS
等の携帯端末装置に接続するカードリーダ装置及びそれ
を用いた認証決済方法に関し、特に販売店に対してカー
ド情報や暗証番号を秘匿したままでカード決済を可能に
する携帯端末接続型のカードリーダ装置及びそれを用い
た認証決済方法に関する。

【0002】

【従来の技術】従来、クレジットカードやキャッシュカ

ードのカード情報を読み込むためのカードリーダ装置を
携帯電話やPHS等の携帯端末に接続して、読み込んだ
カード情報を携帯端末の機能を使ってホストコンピュ
ータに送信してカードによる決済を行うことが知られてい
る。

【0003】従来例としては携帯電話機や業務用無線機
と接続するタイプのカードリーダ装置が、特開平11-
259573号公報に記載されている。この特開平11-
259573号公報に開示された技術では、カードリ
ーダで読み込んだカード情報を、携帯電話機や業務用無
線機の機能を使って送信していた。また携帯端末を使っ
て認証決済処理を行う方法が、特開平11-20335
8号公報に記載されている。

【0004】

【発明が解決しようとする課題】しかしながら、特開平
11-259573号公報に記載されている従来の装置
では、カードリーダ装置で読み込んだカード情報を暗号
化せずに携帯電話機や業務用無線機の機能を使って送信
していた為に、携帯電話機や業務用無線機から発信され
た無線信号を傍受することによりカード情報を盗聴する
ことが可能であるため、カード情報が不正使用される恐
れがあった。

【0005】また特開平11-203358号公報に記
載の販売店に設置されているカードリーダ装置を使用し
た場合には、販売店に設置されているカードリーダ装置
そのものに不正な改造が加えられていた場合、カード情
報や暗証番号の情報の盗聴が可能となり、カード情報が
不正使用される恐れがあった。

【0006】更に、従来の方法では、カード情報や暗証
番号を暗号化していても、同じカード情報や暗証番号か
らは毎回同じ暗号化コードしか生成されないために、カ
ード情報や暗証番号そのものを盗聴することができなく
ても、カード情報や暗証番号から生成された暗号化コー
ドを盗聴することが出来れば、カード情報を不正使用す
ることが可能だった。

【0007】そこで本発明は、カード情報や暗証番号を
販売店に対して秘匿したままで決済処理を行えると共
に、暗号化コードを盗聴されても、盗聴された暗号化コ
ードでは認証処理を行うことが出来ない、セキュリティ
を向上させた携帯端末接続型カードリーダ装置及びそれ
を用いた認証決済方法を提供することを目的とする。

【0008】

【課題を解決するための手段】上述の課題を解決するた
め、本発明の携帯端末接続型カードリーダ装置は、カー
ドに記録されている情報を読み取るカード情報読み取り
部と、暗証番号を入力する入力部と、カード決済を行う
利用者に操作を促すメッセージを表示する表示部と、携
帯電話やPHS等の携帯端末（以下、単に携帯端末と記
す）により暗号化のための公開鍵を受信、あるいは暗号
化したカード情報や暗証番号を携帯端末に送信する通信

部と、この通信部により受信した公開鍵を使ってカード情報及び暗証番号を暗号化する暗号化部とを一体の筐体内に備えることを特徴とする。暗号化部は、暗号化のために使用する公開鍵を一時的に保存しておくためのメモリを備える。本発明における携帯端末接続型カードリーダ装置は、ケーブルにより携帯端末に接続される。

【0009】本発明では、カード情報を管理するホストコンピュータには、カード決済のサービスを提供している販売店の識別情報を管理している管理テーブルを設け、販売店には、それぞれを一意に識別するための識別情報が割り当てられる。

【0010】すなわち本発明は、接続されている携帯端末のデータ通信機能を利用して、クレジットカードやキャッシュカードのデータを管理しているホストコンピュータから暗号化の為に使用する公開鍵を受け取り、受け取った公開鍵を使用して読み込んだカード情報および入力された暗証番号を暗号化し、再び接続された携帯端末のデータ通信機能を利用して、暗号化されたカード情報および暗証番号をホストコンピュータに送り返す機能を有する携帯端末接続型のカードリーダ装置を提供する共に、ホストコンピュータでは、暗号化されたカード情報および暗証番号を公開鍵に対応する秘密鍵を使って復号化し、復号化されたカード情報および暗証番号を使って決済処理を行うことにより、カード情報や暗証番号を販売店に対して秘匿したまま決済処理を行えるようにする。

【0011】さらにカード情報や暗証番号を暗号化する際に使用する公開鍵を毎回更新することにより、決済処理の度に同じカード情報や暗証番号から、毎回異なる暗号化コードを生成し、暗号化コードを盗聴されても、盗聴された一度使われた暗号化コードでは認証処理を行うことが出来ないようにすることで、セキュリティを向上させる。

【0012】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【0013】図1は、本発明の第1の実施の形態を示すブロック図である。図1において、カードリーダ装置1は、クレジットカードやキャッシュカードの情報を読み取るカード情報読み取り部11、暗証番号を入力するための入力部12、カード決済を行うカード利用者（以下カード利用者と記す）に対して操作を促すメッセージを表示する表示部13、読み取ったカード情報や入力された暗証番号を暗号化する暗号化部14、及び携帯端末2を介して外部とデータの送受信をする通信部15が、一体の筐体内に構成される。通信部15は、携帯端末2を介して、クレジットカードやキャッシュカードの情報を管理している信販会社や銀行のホストコンピュータ3（以下ホストコンピュータと記す）から公開鍵を受け取る、あるいは暗号化したカード情報や暗証番号をホスト

コンピュータ3に送る機能を有する。

【0014】カードリーダ装置1と携帯端末2は、ケーブル5で接続される。販売店とホストコンピュータ3との間は、公衆回線6により接続されたコンピュータ等の電子機器4により情報交換が行われる。ホストコンピュータ3と携帯端末2の間は、公衆回線を利用した無線電話網7により接続される。

【0015】カード利用者の携帯端末2には、ホストコンピュータ3から送られた情報を表示するための液晶画面が設けられている。カード決済要求を行う販売店のコンピュータ4には、それぞれの販売店に一意に割り付けられている識別情報が設定されている。ホストコンピュータ3には、カード決済要求を行う販売店のコンピュータ4に割り付けられている識別情報を管理する為の管理テーブル31と、カード利用者の情報を管理する為の管理テーブル32が設けられている。カード利用者の情報管理テーブル32には、カード利用者のカード情報、暗証番号、及びカード決済に必要な情報が格納されている。

【0016】図2は、本発明における各装置間の決済処理の流れを示す図である。図3は、カード情報を管理しているホストコンピュータ3において、カード利用者の携帯端末2から送られてきた暗号化されたカード情報及び暗証番号を使った認証方法で使われるデータ処理方法を示す概略図である。図4、5は、本発明による決済処理において、ホストコンピュータ3で行われる決済処理の流れを示すフローチャートであり、図6、7は、カード利用者の携帯端末2側で実行される処理の流れを示すフローチャートである。

【0017】本発明では、カード利用者がカードを利用して販売店で商品を購入する際には、図2において自分の携帯端末2の電話番号とクレジットカードを発行した信販会社、あるいはキャッシュカードを発行した銀行の名称を、電話、電子メール、口頭、FAX等の手段により販売店に教える。販売店では、コンピュータ4を使って、カード利用者の携帯端末の電話番号と商品の代金と販売店のコンピュータ4に割り当てられた識別情報を、カードを発行した信販会社あるいは銀行のホストコンピュータ3に送信して決済要求（201）を行う。

【0018】ホストコンピュータ3は、販売店のコンピュータ4から決済要求を受信すると（図4のS1）、受信した決済要求（201）から販売店のコンピュータに割り当てられた識別情報を取り出し、この識別情報をキーにして販売店の識別情報管理テーブル31を検索する（S2）。決済要求（201）を行った販売店の識別情報が、識別情報管理テーブル31に登録されていなかった場合（S3でNの場合）には、ホストコンピュータ3は販売店からの決済要求（201）を破棄し、販売店のコンピュータ4に対して決済不履行を通知して処理を終える（S9）。

【0019】販売店の識別情報が識別情報管理テーブル31に登録されていた場合（S3でYの場合）には、ホストコンピュータ3は決済要求（201）からカード利用者の携帯端末2の電話番号を取り出して、携帯端末2に電話をかけて、携帯端末2に対して販売店から請求されている商品代金の金額、及び販売店の情報を送信して決済要求（202）を行う（S4）。

【0020】カード利用者の携帯端末2は、ホストコンピュータ3から決済要求（202）を受け取ると（図6のS31）、決済要求（202）から商品の金額と販売店の情報を取り出して、携帯端末2の液晶画面に表示し、カード利用者に対して決済要求を承認するか拒絶するかを促すメッセージを液晶画面に表示して、カード利用者が携帯端末2のキー操作を行うのを待つ。カード利用者が携帯端末2のキー操作を行って決済要求を拒絶した場合（S32でNの場合）、あるいは携帯端末2が液晶画面に決済要求を承認するか拒絶するかを促すメッセージを表示してから一定時間経過しても携帯端末2のキー操作が行われなかった場合には、携帯端末2はホストコンピュータ3に対して決済要求拒絶応答を送信して（S46）、ホストコンピュータ3との間の接続を切断する。

【0021】ホストコンピュータ3は、カード利用者の携帯端末2に対して決済要求205を送信してから、一定時間内にカード利用者の携帯端末2から決済要求承認応答を受信出来なかった場合（図4のS5でNの場合）、販売店のコンピュータ4に対して決済不履行を通知して処理を終了する（S9）。

【0022】カード利用者が携帯端末2のキー操作を行って決済要求を承認した場合（図6のS32でYの場合）は、携帯端末2はホストコンピュータ3に対して決済要求承認応答を返す（S33）。

【0023】ホストコンピュータ3は、カード利用者の携帯端末2に対して決済要求を送信してから一定時間以内に携帯端末2から決済要求承認応答を受信した場合（図4のS5でYの場合）、公開鍵暗号方式で暗号化を行う際に使用する公開鍵（301）と秘密鍵（302）の組を生成（203）して（S6）、カード利用者の携帯端末2に公開鍵（301）を送信（204）する（S7）。

【0024】カード利用者の携帯端末2に公開鍵（301）を送信してから一定時間以内に、カード利用者の携帯端末2から暗号化されたカード情報を受信出来なかった場合（S8でNの場合）には、ホストコンピュータ3は、販売店のコンピュータ4に対して決済不履行を通知して処理を終了する（S9）。

【0025】ホストコンピュータ3から公開鍵を受信（204）したカード利用者の携帯端末2は（図6のS34）、カードの読み取りを促すメッセージを作成し、メッセージと公開鍵をケーブル接続されているカードリ

ード装置1に送る。携帯端末2からメッセージと公開鍵を受信したカードリーダ装置の通信部15は、公開鍵を暗号化部14のメモリに格納し、メッセージを表示部13に送って表示し、カード利用者がカードを読み取らせるのを待つ。カード情報読み取り部11でカード情報の読み取り（205）を行うと（S35）、読み取られたカード情報は暗号化部14に送られ、暗号化部のメモリに格納されている公開鍵を使って公開鍵暗号方式により暗号化（206）される（S36）。暗号化部14により暗号化されたカード情報は、通信部15を介して携帯端末2に送られる。

【0026】ケーブル接続されているカードリーダ装置1から暗号化されたカード情報を受信した携帯端末2は、データ通信機能を使って暗号化されたカード情報をホストコンピュータ3に送信（207）する（S37）。

【0027】図3において、カード利用者の携帯端末2から暗号化されたカード情報303を受信したホストコンピュータ3は、暗号化されたカード情報303のコピー304を作成してメモリに保存する。次にホストコンピュータ3は、カード利用者の携帯端末2に送った公開鍵301に対応する秘密鍵302を使って、暗号化されたカード情報303を復号化（208）して、平文化されたカード情報305を得る（図4のS10）。次にホストコンピュータ3は、平文化されたカード情報305を公開鍵301で再度暗号化して暗号化されたカード情報306を得る。このようにして暗号化されたカード情報306と、カード利用者の携帯端末から送られた暗号化されたカード情報のコピー304を比較する（S11）。

【0028】暗号化されたカード情報304と306が一致しなかった場合（S12でNの場合）には、ホストコンピュータ3は、カード利用者の携帯端末2と販売店のコンピュータ4の両方に決済不履行通知を送信して接続を切断し、決済処理を終了する（S13）。

【0029】暗号化されたカード情報304と306が一致した場合（S12でYの場合）には、ホストコンピュータ3は、平文化したカード情報305をキーにして、カード利用者の情報管理テーブル32を検索する（S14）。平文化されたカード情報305がカード利用者の情報管理テーブル32に登録されていなかった場合（S15でNの場合）には、ホストコンピュータ3は、カード利用者の携帯端末2と販売店のコンピュータ4の両方に決済不履行通知を送信して接続を切断し、決済処理を終了する（S27）。

【0030】ホストコンピュータ3から決済不履行通知を受信したカード利用者の携帯端末2は（図7のS38でYの場合）、受信した決済不履行通知をケーブル接続されているカードリーダ装置1に送信して、ホストコンピュータ3との間の接続を切断する。決済不履行通知を

受け取ったカードリーダ装置1は、暗号化部14のメモリに格納されている暗号化の為の公開鍵を破棄して(S45)全ての処理を終了する。

【0031】平文化したカード情報305がカード利用者の情報管理テーブル32に登録されていた場合(図5のS15でYの場合)には、ホストコンピュータ3は、平文化したカード情報305をメモリに保存して、カード利用者の携帯端末2に対して暗証番号の入力要求を送信(S16)して、カード利用者の携帯端末2からの応答を待つ。

【0032】ホストコンピュータ3から暗証番号の入力要求を受信(図7のS39)したカード利用者の携帯端末2は、暗証番号の入力を促すメッセージを作成し、ケーブル接続されているカードリーダ装置1に送る。携帯端末2から暗証番号の入力を促すメッセージを受信したカードリーダ装置1は、メッセージを表示部13に送って表示し、カード利用者が暗証番号を入力するのを待つ。入力部12により入力された暗証番号(205)は暗号化部14に送られ、暗号化部14のメモリに格納されている公開鍵を使って公開鍵暗号化方式により暗号化(206)される(S41)。暗号化部14により暗号化された暗証番号は、通信部15を介して携帯端末2に送られる。

【0033】ケーブル接続されているカードリーダ装置1から暗号化された暗証番号を受信した携帯端末2は、データ通信機能を使って暗号化された暗証番号をホストコンピュータ3に送信(207)する(S42)。

【0034】ホストコンピュータ3は、カード利用者の携帯端末2に暗証番号の入力要求を送信してから一定時間以内に暗号化された暗証番号を受け取ることが出来なかった場合(図5のS17でNの場合)、カード利用者の携帯端末2と販売店のコンピュータ4の両方に対して決済不履行通知を送信して(S27)、接続を切断し全ての処理を終了する。

【0035】図3において、ホストコンピュータ3は、カード利用者の携帯端末2に暗証番号の入力要求を送信してから、一定時間以内にカード利用者の携帯端末2から暗号化された暗証番号307を受信した場合(S17でYの場合)、暗号化された暗証番号307のコピー308を作成してメモリに保存する。次にホストコンピュータ3は、カード利用者の携帯端末2に送った公開鍵301に対応する秘密鍵302を使って、暗号化された暗証番号307を復号化(208)して、平文化された暗証番号309を得る(S18)。次にホストコンピュータ3は、平文化された暗証番号309を公開鍵301で再度暗号化して暗号化された暗証番号310を得る。このようにして暗号化された暗証番号310と、カード利用者の携帯端末2から送られた暗号化された暗証番号のコピー308を比較する(S19)。

【0036】暗号化された暗証番号310と、受信した

暗号化された暗証番号のコピー308が一致しなかった場合(S20でNの場合)には、ホストコンピュータ3は、カード利用者の携帯端末2と販売店のコンピュータ4の両方に決済不履行通知を送信(S27)して接続を切断し、決済処理を終了する。

【0037】暗号化された暗証番号310と、受信した暗号化された暗証番号のコピー308が一致した場合(S20でYの場合)には、ホストコンピュータ3は、メモリに保存しておいた平文化したカード情報305と、平文化された暗証番号309を使って、カード利用者の情報管理テーブル32を検索する(S21)。管理テーブル32からカード情報305に対応する暗証番号を取り出し、平文化された暗証番号309と比較する。

【0038】管理テーブル32から取り出したカード情報305に対応する暗証番号と、平文化された暗証番号309が一致しなかった場合(S22でNの場合)には、ホストコンピュータ3は、カード利用者の携帯端末2と販売店のコンピュータ4の両方に決済不履行通知を送信(S27)して接続を切断し、決済処理を終了する。

【0039】管理テーブル32から取り出したカード情報305に対応する暗証番号と、平文化された暗証番号309が一致した場合(S22でYの場合)には、決済処理(209)を行う(S23)。

【0040】決済処理が完了したら、ホストコンピュータ3は、カード利用者の携帯端末2と販売店のコンピュータ4の両方に決済処理の完了通知(210、211)を送信(S24)して接続を切断し(S25)、使用済みになった公開鍵301、秘密鍵302の組、暗号化されたカード情報303、304、306、平文化されたカード情報305、及び暗号化された暗証番号307、308、310、平文化された暗証番号309を全て破棄(213)して(S26)、全ての決済処理を終了する。

【0041】図2において、ホストコンピュータ3から決済処理の完了通知(210)を受信したカード利用者の携帯端末2は、決済処理の完了通知(210)をカードリーダ装置1に送る。決済処理の完了通知を受信したカードリーダ装置1は、暗号化部14のメモリに保存されている公開鍵を破棄(212)して(図7のS45)、全ての決済処理を終了する。

【0042】図2において、ホストコンピュータ3から決済処理の完了通知(211)を受信した販売店のコンピュータ4は、決済処理の完了を確認して全ての決済処理を終了する。

【0043】

【発明の効果】以上説明したように、本発明によれば、販売店に備え付けられているカードリーダ装置を利用することなく決済処理を行うことが出来る。従って、ICカードや磁気カードのように、カード情報の読み取り方

式の違うカードリーダ装置を販売店に設置する必要はなくなる。

【0044】また、カード利用者のカード情報や暗証番号を、販売店に対して秘匿したままでカード決済を行うことが出来るので、販売店に備え付けられているカードリーダ装置に不正な改造が加えられていても、カード利用者のカード情報や暗証番号が盗まれることはなくなる。

【0045】また、カード利用者の携帯端末から送信される暗号化されたカード情報や暗証番号は、カードを発行した信販会社あるいは銀行のホストコンピュータ内に秘匿された秘密鍵によってのみ、元のカード情報及び暗証番号に平文化することが出来るので、携帯端末から発信される電波が盗聴されても、暗号化されたカード情報や暗証番号を元のカード情報や暗証に復元することが出来ない。従ってカード利用者の携帯端末から発信される電波が盗聴されても、カード利用者のカード情報や暗証番号が盗まれることはなくなる。

【0046】更に、ホストコンピュータによって配布される公開鍵は毎回異なるので、公開鍵を使ってカード情報や暗証番号を暗号化した結果、生成される暗号化コードは毎回異なるものになる。従って、一度使われた暗号化コードでは決済処理を行うことが出来ないので、悪意のある利用者が、他人の携帯端末から発信される暗号化されたカード情報や暗証番号の情報を傍受・盗聴して、次のホストコンピュータとの接続時に携帯端末から盗聴した暗号化されたカード情報や暗証番号の情報を送っても、ホストコンピュータ側で持っている秘密鍵は更新されているので、ホストコンピュータ側では復号化して元のカード情報や暗証番号を得ることが出来ない。そのため暗号化された他人のカード情報や暗証番号を盗聴しても、決済処理を行うことは出来ない。

【図面の簡単な説明】

【図1】本発明におけるカードリーダ装置及びカード情報を管理するホストコンピュータの実施の形態を示すブロック図。

【図2】本発明におけるカード決済処理の流れを示す説

明図。

【図3】本発明における暗号化されたカード情報及び暗証番号を使った認証処理で使われるデータを示す概略図。

【図4】本発明においてカード情報を管理するホストコンピュータで実行される処理の流れを示すフローチャート。

【図5】本発明においてカード情報を管理するホストコンピュータで実行される処理の流れを示すフローチャート。

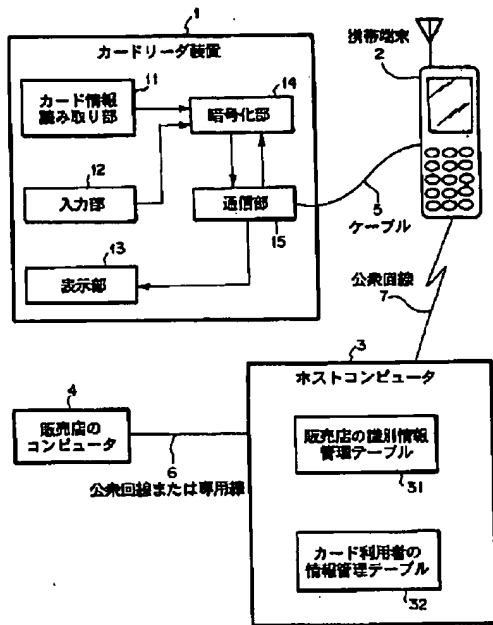
【図6】本発明においてカード利用者の携帯端末及びカードリーダ装置で実行される処理の流れを示すフローチャート。

【図7】本発明においてカード利用者の携帯端末及びカードリーダ装置で実行される処理の流れを示すフローチャート。

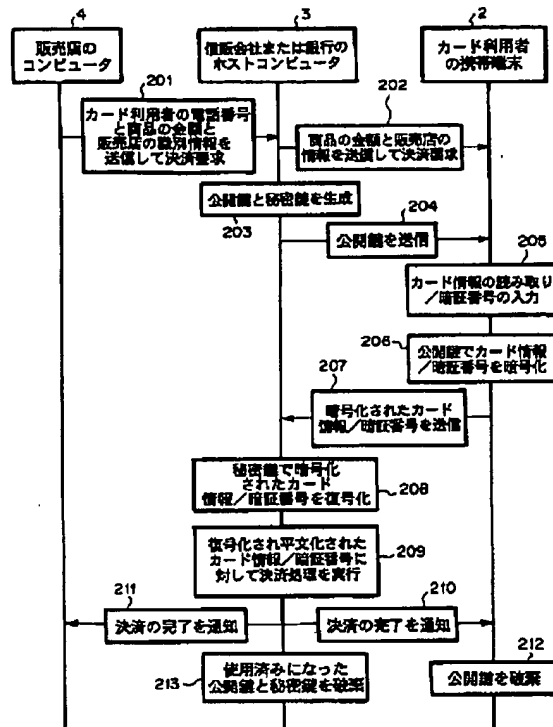
【符号の説明】

- 1 カードリーダ装置
- 2 携帯端末
- 3 ホストコンピュータ
- 4 販売店のコンピュータ
- 5 ケーブル
- 6 公衆回線または専用線
- 7 公衆回線
- 11 カード情報読み取り部
- 12 入力部
- 13 表示部
- 14 暗号化部
- 15 通信部
- 31 販売店の識別情報管理テーブル
- 32 カード利用者の情報管理テーブル
- 301 公開鍵
- 302 秘密鍵
- 303, 304, 306 暗号化されたカード情報
- 305 平文化されたカード情報
- 307, 308, 310 暗号化された暗証番号
- 309 平文化された暗証番号

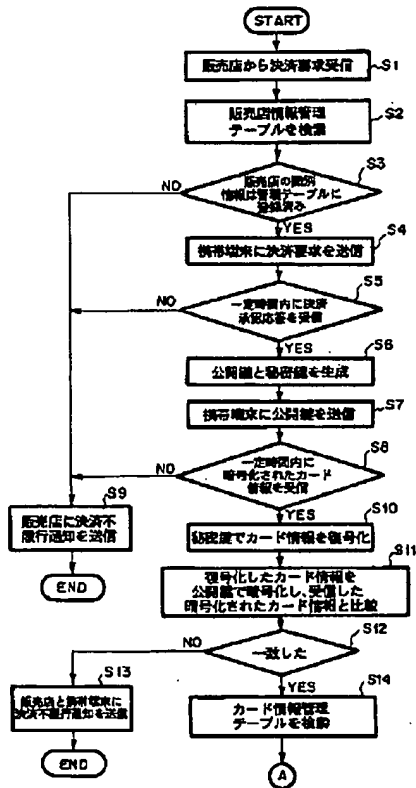
【図1】



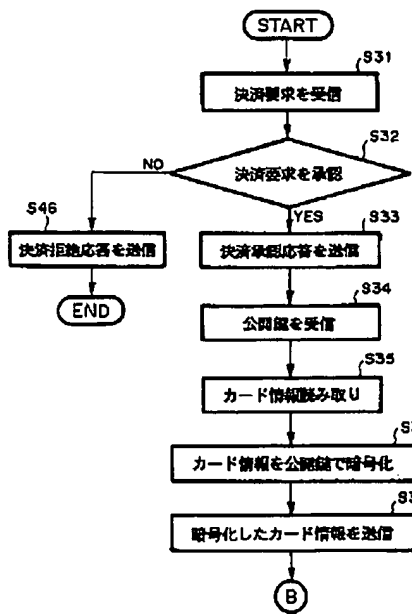
【図2】



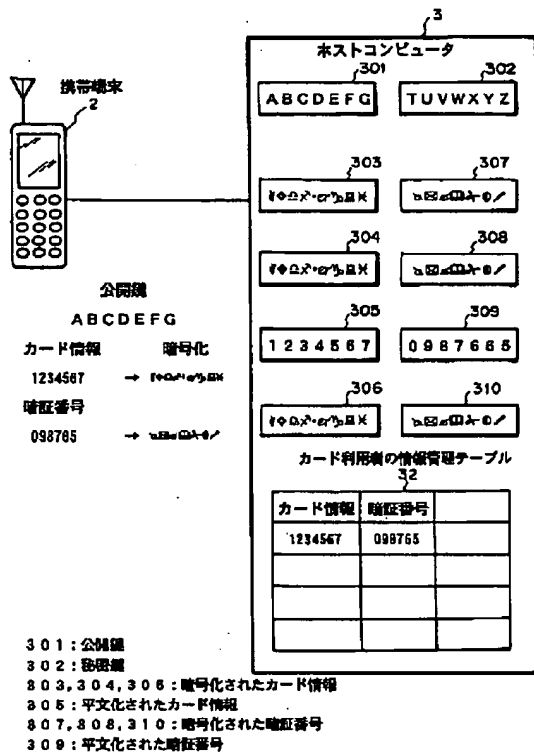
【図4】



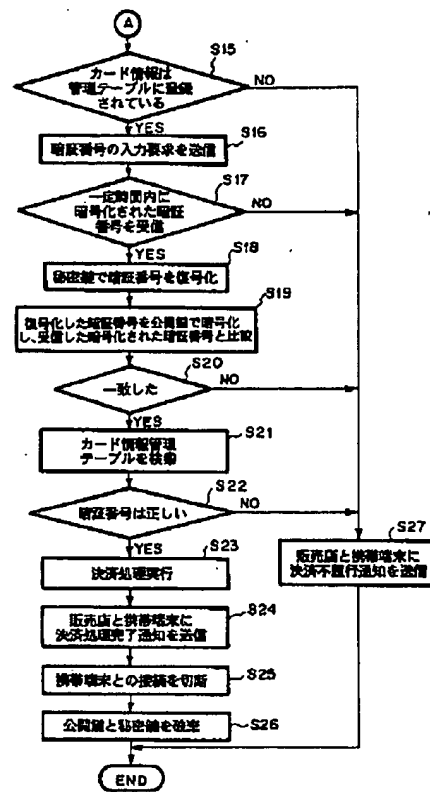
【図6】



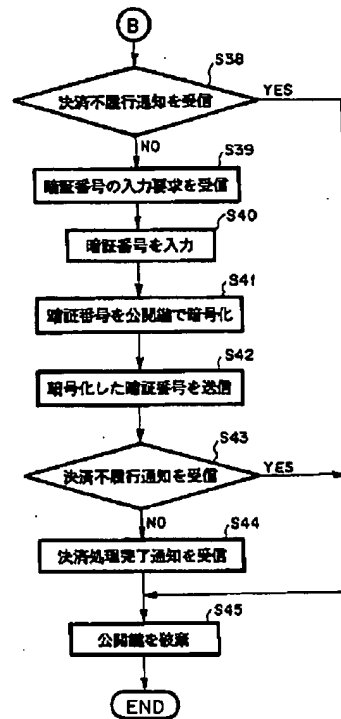
【図3】



【図5】



【図7】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	テマート ¹ (参考)
G 0 6 F 17/60	5 0 6	G 0 6 F 17/60	5 0 6
	5 1 2		5 1 2
G 0 6 K 17/00		G 0 6 K 17/00	S
G 0 7 F 7/10		G 0 7 F 7/10	
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 A
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
			6 0 1 F